

REMARKS

Claims 1-22 are currently pending in the patent application. The Examiner has finally rejected Claims 1-6, 21 and 22 under 35 USC 102 as anticipated by Miller; and, has rejected Claims 7-20 under 35 USC 103 as unpatentable over Miller in view of Isaacman. The Examiner has indicated, in the **Response to Arguments** section, that Applicants have pointed out features of the claimed invention that differ from Miller; but, that the claims do not reflect the differences. Accordingly, Applicants have amended the claims to more explicitly recite those differences. Applicants believe that the claims, as amended, are patentable over the cited art.

The present invention teaches a method, system, and program storage device for enabling a security function for a computer, wherein a security device is optionally attached to the computer and wherein, when a security device is attached, the use of the computer can be selectively enabled. In a first embodiment of the invention, to which Claims 1, 2, 5, 7, 9, 11, 14, 16, 18, 20 and 22 are directed, a detect enable bit is stored at a first storage location in the computer, wherein the detect enable bit setting designates subsequent processing relative to a

JP919990035

security device/function. After the detect enable bit has been set, the computer detects whether a security device is attached and sets an attachment bit in a second storage location of the computer accordingly. The detection can be done continually, when the computer is powered up, or when the computer enters an energy-saving mode. The computer will subsequently use the setting data and attachment data to detect removal of a security device. If a security device has been removed, and the attachment data (a.k.a., the security device history bit) indicates that a security device should be there, access to the computer is prohibited. In a further embodiment of the invention, to which Claims 3, 4, 6, 8, 10, 12, 13, 15, 17, 19 and 21 are directed, the connection of a lithium battery or the like, or the conduction of the power line of the internal basic power supply is carried out based on setting data. This conduction is enabled by connection means such as an analog switch. With this, even for a computer having no security function, the internal basic supply is not shut down. Disconnection is performed when the power line of the internal basic power supply is formed by the security device, and after the security device is once attached and the system recognizes that this computer is a computer having a security function. This is because the internal

JP919990035

-10-

basic power supply is not disconnected even if the connection is released, since the power line of the internal basic power supply is formed by the security device. If the security device is removed, and if it is unauthorized access to the computer, the power line of the internal basic power supply is disconnected, and the one within the computer which is supplied with power from the internal basic power supply is initialized, so access to the computer is prohibited. Applicants respectfully assert that the invention is patentable over the cited prior art.

The Miller patent is cited as anticipating Claims 1-6, 21 and 22, and is cited in conjunction with the Isaacman patent in rejecting Claims 7-20 as obvious. The Miller patent is directed to a system and method for providing a security key device which is not a part of the computer and which must be coupled to the computer bus in order for the computer to be operational. Miller teaches that the security key includes a connector which is coupled to the bus, a controller, and a storage device coupled to the controller. A unique key code is stored in the security key along with an encrypted password. In order for the computer to operate when the security key device is coupled to the computer, the key code stored in the security key must match the key code stored in the computer. Further, a password

JP919990035

-11-

entered into the computer is encrypted by the security key and must match the encrypted password stored in the security key to enable computer operation.

Applicants respectfully assert that the Miller patent does not anticipate each and every claim feature of the present invention. With specific reference to the claim language, Claim 1 recites a method for prohibiting access to a computer after a security device attached to said computer is removed, comprising the steps of (a) storing setting data comprising a detect enable bit for establishing the computer settings with respect to the attachment of a security device to said computer in a first storage unit of said computer; (b) detecting the attachment of the said security device to said computer after said step (a) and during one of the power-on and the energy-saving mode of said computer; (c) storing the attachment data comprising a security device history bit indicating the detection in step (b) in a second storage unit equipped in said computer; (d) detecting a removal of said security device from said computer based on said previously-stored setting data and said attachment data; and (e) prohibiting access to said computer in response to the detection in said step (d). With respect to the first step of storing setting data comprising a detect enable bit for establishing the computer settings with

JP919990035

-12-

respect to the attachment of a security device to the computer in a first storage unit of said computer, Applicants note that the Miller patent does not store such setting data in a first storage unit of the computer. The only thing which Miller stores in the computer is a security key. The Miller security key is not a setting which designates to the computer how to proceed with processing relative to the attachment of a security device. Under the Miller teachings, processing can be conducted in only one way. Miller does not teach or suggest that the process flow can be set differently with respect to a security device. In fact, Miller expressly states in the Abstract that the connector of the security key **must** be coupled to the computer bus for the computer to be operational. Applicants have amended the language of independent Claims 1, 5, and 22 to more clearly recite the storing of the setting data.

With respect to the second claim feature of detecting the attachment of the security device to the computer after storing the setting data and during one of the power-on and the energy-saving mode of said computer, Applicants assert that Miller does not teach the claimed step. The Examiner has stated that the claimed step is "met by comparing the code stored in the security key with the key code stored in the computer". Applicants respectfully assert that a

JP919990035 -13-

security device must first be detected before a key code from that device can be compared to a key code stored in the computer. Clearly the cited Miller teachings from the Abstract and block 84 of Fig. 5 do not anticipate detecting attachment of a security device during power-on or during entry into an energy-saving mode.

With regard to the claim feature of storing the attachment data comprising the security device history bit indicating detection of attachment of a security device in a second storage unit of the computer, Applicants respectfully disagree with the Examiner's assertion that the claim language is anticipated by the Miller teachings of the key code received from the key 40 being compared to the key code stored in the BIOS flash 24. The key code stored by the computer is stored in one storage location. Whether it is moved into another place for comparison does not change the fact that it is stored in one location. Further, the key code is one value stored at one location. The claim recites a first value, the setting data comprising the detect enable bit, being stored at a first location and a second value, the attachment data comprising the security device history bit, being stored at a second location. Clearly, the Miller patent does not anticipate that recitation.

JP919990035

-14-

Applicants reiterate that the Examiner has cited the comparison of the key codes against two distinct steps of the present invention. Applicants respectfully assert that the comparing of the key codes cannot anticipate both a detecting step and a storing step. The Examiner did not respond to this argument in the final office action.

With respect to the claim step of detecting removal of the security device from the computer based on the previously-stored setting and attachment data, the Examiner has concluded that Miller anticipates that claim language by its illustration in Fig. 7 that, once removal of the security key is detected, the computer is put out of operational mode. The present invention detects that a security device has been removed based on its stored setting data, which tells the computer what attachment-related steps to follow, and based on the stored attachment data, which tells the most recent history of detected attachment of a security device. Miller simply detects the presence or absence of a security device. Miller does not detect **removal** of a security device based on previously-stored data. Moreover, Miller simply puts the computer out of operational mode when it detects the absence of a security device. In contrast, the present invention will only execute the step of prohibiting access to the computer if

JP919990035 -15-

removal is detected, and removal is only detected relative to stored setting data and historical data (Claim 1) or stored setting data and historical data in conjunction with entry of a password (Claim 2). The present invention can grant access if a security device is not there, provided that its stored data indicates that it should not expect to find a security device. The present invention is far more robust than the Miller system.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Miller patent does not teach the storing of setting data comprising a detect enable bit for establishing the processing settings relative to attachment of a security device in a first computer storage location, does not teach detecting attachment and storing attachment data comprising a security device history bit in a second computer storage location, does not teach detecting removal of a security device based on previously-stored information, and does not teach prohibiting access based on the historically-based detection, it cannot be maintained that Miller anticipates the invention as set forth in the independent claims, Claims 1, 3, 5, 6, 21 and 22, or the claims which depend therefrom and add further limitations thereto.

JP919990035

-16-

Applicants further assert that the Miller patent does not anticipate the claim language as set forth in Claims 3, 4, 6, 8, 10, 12, 13, 15, 17, 19, and 21. With specific reference to the language of independent Claim 3, the claim features include the steps of storing setting data for setting the attachment of a security device to the computer in a first storage unit equipped in the computer; connecting the connection device of an internal basic power wiring equipped in said computer after step (a) based on the stored setting data, thereby to secure a power line, (c) disconnecting the connection device while the security device is attached to the computer to form the power line of the internal basic power supply; (d) allowing access to said computer when said security device comprises the power line of said internal basic power supply and maintaining said disconnection in said step (c) and (e) if the security device is removed, prohibiting access to the computer by the disconnection. In rejecting Claims 3-4 and 6, the Examiner has stated that "Miller explicitly shows disconnection causes computer to go into a sleep mode" and has stated that "it is inherent to store data while main power supply of the computer is as at a halt and a backup power supply is operating". Applicants have previously noted that Miller expressly teaches that removal of a security key causes the

JP919990035

-17-

computer to be put out of operation. Miller does not teach that "disconnection" causing the computer to go into sleep mode. The cited step at 160 of Fig. 6 of Miller, as taught in the Specification, refers to the Miller computer going into sleep mode if a non-matching key code is entered. Clearly those Miller teachings do not anticipate the invention as claimed.

With respect to the rejection of Claims 5 and 6, Applicants note that Claim 5 does not recite storing data while a main power supply is "as at a halt" as the Examiner contends. The language of Claim 5 parallels that of Claim 1 which has been defended above. Further, Claim 6 does not recite storing data while a main power supply is at a halt and a backup power supply is operating. What Claim 6 recites is means for performing the step of connecting a connection device of an internal basic power supply based on stored setting data, the setting data having been stored relative to attachment of a security device to the computer. Applicants again argue that Miller does not teach or suggest the storing of setting data, as claimed, and does not teach or suggest using that setting data for connecting a connection device to secure a power supply line. Moreover, Miller clearly does not teach the remaining steps, which are not expressly rejected by the Examiner.

JP919990035

-18-

Applicants again assert that a reference does not anticipate claim language under 35 USC 102 if the reference does not teach each and every claim step. Since the Miller patent does not teach storing and maintaining setting data, connecting a connection device based on the setting data, disconnecting the connection device while a security device is attached to the computer, and maintaining disconnection and prohibiting access by the disconnection, it cannot be maintained that Claims 3, 4, 6 and 21 are anticipated by the Miller patent teachings.

The Examiner has acknowledged that the Miller patent does not teach the use of RFID tags. The Examiner has cited the Isaacman patent as teaching a conventional RFID tag system. Applicants respectfully assert that the additional of the Isaacman RFID teachings to the Miller patent would not render the pending claims obvious. If one were motivated to modify Miller to include the Isaacman teachings, one would provide an RF antenna as the connector of the security key which would be coupled to the bus of the computer. Such a modification would not result in the invention as claimed, since neither Miller nor Isaacman teaches or suggests the claim features of storing setting data for setting the attachment of a security device to the computer or of using the setting data in conjunction with

JP919990035

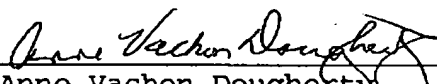
-19-

detected attachment data for detection of removal of a security device (Claims 1, 2, 5, 7, 9, 11, 14, 16, 18, 20 and 22) or of using the setting data for connecting a connection device of an internal basic power wiring thereby to secure a power supply line (Claims 3, 4, 6, 8, 10, 12, 13, 15, 17, 19, and 21). Applicants respectfully conclude that the Examiner has not made out a *prima facie* case of obviousness since the cited references do not teach or suggest all of the claim limitations (*In re Wilson*, 424 F. 2d 1382, 165 U.S.P.Q. 494 (C.C.P.A. 1970)).

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

H. Horikoshi, et al

By: 
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910